Subject: A reminder of the importance of Business Associate agreements
Date: Wednesday, March 30, 2016 11:40:38 AM

Wider HIPAA audits may drive stronger vendor contracts

By Joseph Conn | March 23, 2016

The volume of patient data handled by vendors of healthcare organizations has exploded with the near ubiquity of electronic health records systems and the growing role of analytics and mobile devices in healthcare.

The feds appear to be preparing to clamp down on the sometimes porous flow of patient data handled by contractors, whose security failures have been linked to the exposure of nearly 33 million individuals' medical records since 2009.

These contractors, termed “business associates” under HIPAA, will be included as primary audit targets in the second round of HIPAA audits by HHS' Office for Civil Rights.

“There are so many people who are doing innovations and startups and want to get into healthcare and are unaware of the rules and regulations,” said David Muntz, former principal deputy director of the Office of the National Coordinator on Health Information Technology at HHS. Muntz now heads a Dallas consulting firm. “What I'm hoping it will do is keep people out who are insincere about becoming HIPAA-compliant.”

Some larger healthcare organizations have employed hundreds and in some cases as many as a thousand business associates, according to Adam Greene, a partner in the Washington, D.C., office of Davis Wright Tremaine.

In one sense, by including the business associates, the civil rights office is simply catching up with privacy and security rules it issued three years ago. But the OCR announcement also means that enforcement of these more stringent rules could give healthcare organizations more leverage to get stronger agreements with their contractors.

“It will force greater visibility into what's going on--and greater accountability,” said Michael Overly, a partner at Foley & Lardner, who specializes in cybersecurity law. “In many instances, covered entities don't have the right to go in and audit what a business associate is doing,” particularly some of the biggest cloud vendors, which severely restrict access to their data centers, Overly said.

But now that BAs are legally liable to the feds for compliance with HIPAA privacy and security rules, “covered entities will insist on having some kind of audit rights” when they sign HIPAA-mandated agreements with these vendors, Overly said.

Upgrades to the HIPAA privacy and security rules in the health IT provisions of the American Recovery and Reinvestment Act of 2009 puts BAs on an equal legal footing with

HIPAA covered entities – hospitals, physician practices, health plans and claims clearinghouses. That means vendors that violate the rules are subject to civil monetary penalties of up to $1.5 million a year.

“A significant part of the (first-round) audit process,” completed in late 2013, included OCR hiring a contractor “to come up with the number of covered entities out there,” Green said. “I've heard the figure of 3 million.”

One goal of the new round of audits, Greene said, will be to assemble a sort of directory of business associates.

The first phase will involve OCR staff and special hires conducting “desk audits,” not requiring agents to go into the field. Covered entities will be asked to provide basic information about their business associates. “It won't be a complete list,” Green said, but it will provide a starting point for identifying business associates to audit.

Just as business associates now share equal legal liability under HIPAA, they've long shared culpability for data breaches, according to federal records.

Of the 1,472 major healthcare data breaches on the OCR's “wall of shame” website, 309 (21%) involved a business associate. Those breaches exposed 32.8 million individuals' records. The wall displays breach information going back to September 2009.

Last week, the civil rights office announced reaching a $1,550,000 settlement agreement with Memorial Health Care, Robinsdale, Minn., over possible HIPAA violations, which included not having a business associate's agreement with Accretive Health, a Chicago-based revenue cycle management firm.

Last summer, Systema Systems, a Larkspur, Calif.-based provider of claims management software, moved a copy of a database to Amazon Web Services, a major cloud data storage provider, but without controls needed to block unauthorized users.

A Texas computer hobbyist downloaded them. Government agencies in Kansas, Utah and California learned about the breach when the hobbyist called and told them that copies of their workers' compensation and liability insurance records on about 1.5 million people were on his computer hard drive.

Overly said the Systema breach could be a poster child for what could go wrong with covered entity/business associate relationships. “That's exactly the thorny problem that's presented to many healthcare providers,” Overly said. “I know who I'm talking to, but I don't know who they're contracting with.”

If a vendor decides to subcontract its work, “you need to make sure that the subcontracting party is bound by the (business associate) agreement,” Overly said.